UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,062	12/30/2003	Daryl Carvis Cromer	RPS20030216US1	8316

36491 7590 12/17/2007

Kunzler & McKenzie
8 EAST BROADWAY
SUITE 600
SALT LAKE CITY, UT 84111

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
12/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Supplemental Notice of Allowability	Application No. 10/748,062	Applicant(s) CROMER ET AL.	
	Examiner Ellen C. Tran	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *26 November 2007*.

2. ☒ The allowed claim(s) is/are *1-3,5-7,9-13,15-19 and 21-29*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *6 December 2007* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Ellen Tran
ELLEN TRAN
PATENT EXAMINER
ART 2134

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Brian Kunzler on 6 December 2007.

Conclusion

2. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen. Tran
Patent Examiner
Technology Center 2134
8 December 2007

EXAMINER'S AMENDMENT

Please amend the claims as indicated.

1. (Previously Presented) An apparatus for secure computer readable medium backup, the apparatus comprising:

a computer readable medium having at least a first accessible portion and a second encrypted portion; and

a trusted platform interface module operatively coupled with the computer readable medium and configured to communicate with a cryptographic module, wherein the trusted platform interface module comprises a password module, the trusted platform interface module initializing the password module in response to verifying the cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module, the password module configured to store and transmit an encrypted password to the cryptographic module, and receive an unencrypted password from the cryptographic module.

2. (Original) The apparatus of claim 1, wherein the cryptographic module comprises a trusted platform module (TPM).

3. (Original) The apparatus of claim 1, wherein the computer readable medium comprises a computer readable peripheral selected from the group consisting of a hard disk drive, a universal serial bus storage device, a floppy disk, an optical storage disk, a flash memory storage device, and a network attached storage drive.

4. (Canceled)

5. (Currently amended) The apparatus of claim [[5]]1, wherein the encrypted password comprises a unique password configured to be decrypted by the cryptographic module that first created the encrypted password.

6. (Original) The apparatus of claim 1, wherein the computer readable medium module further comprises a backup utility module configured to selectively copy data from a storage device source, detect newer versions of data stored on the storage device source, and replace older versions of the data on the computer readable medium with newer versions of the data.

6. (Previously Presented) A device for secure computer readable medium backup, the device comprising:

a motherboard;

a cryptographic module coupled to the motherboard and configured to communicate with a computer readable medium; and

the computer readable medium comprising a trusted platform interface module configured to communicate with the cryptographic module, wherein the trusted platform interface module comprises a password module, the trusted platform interface module initializing the password module in response to verifying the cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module, the password module configured to store and transmit an encrypted password to the cryptographic module, and receive an unencrypted password from the cryptographic module.

8. (Canceled)

9. (Previously Presented) The device of claim 7, wherein the cryptographic module is configured to receive the encrypted password from trusted platform interface module, decrypt the password, and transmit the decrypted password to the trusted platform interface module.

10. (Previously Presented The device of claim 7, wherein the cryptographic module comprises a TPM.

11. (Currently amended) The device of claim 7, wherein the motherboard further comprises a memory and a processor coupled to the memory.

12. (Original) The apparatus of claim 7, wherein the computer readable medium comprises a computer readable peripheral selected from the group consisting of a hard disk drive, a universal serial bus storage device, a floppy disk, an optical storage disk, a flash memory storage device, and a network attached storage drive.

13. (Previously Presented) A system for secure computer readable medium backup, the system comprising:
a motherboard;
a cryptographic module coupled to the motherboard configured to decrypt encrypted passwords;
a computer readable medium module having at least a first accessible portion and a second encrypted portion; and
a trusted platform interface module operatively coupled with the computer readable media module and configured to communicate with the cryptographic module, wherein the trusted

platform interface module comprises a password module, the trusted platform interface module initializing the password module in response to verifying the cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module, the password module configured to store and transmit an encrypted password to the cryptographic module, and receive an unencrypted password from the cryptographic module.

14. (Canceled)

15. (Original) The system of claim 13, wherein the encrypted password is configured to be decrypted by the cryptographic module that first created the encrypted password.

16. (Original) The apparatus of claim 13, wherein the computer readable medium further comprises a backup utility configured to selectively copy data from a storage device source, detect newer versions of data stored on the storage device source, and replace older versions of the data on the computer readable medium module with newer versions of the data.

17. (Previously Presented) A computer readable storage medium comprising computer readable code configured to carry out a method for secure computer readable medium backup, the method comprising:

providing a computer readable medium having at least a first accessible portion and a second encrypted portion;

initializing a password module in response to a cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register

value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module;

transmitting an encrypted password to the cryptographic module;

authenticating the encrypted password;

decrypting the encrypted password;

transmitting the decrypted password to the computer readable medium module; and

decrypting the second encrypted portion using the decrypted password.

18. (Original) The computer readable storage medium of claim 17, wherein the method further comprises copying data from a source storage device, and storing the data in the second encrypted portion of the computer readable medium.

19. (Original) The computer readable storage medium of claim 17, wherein the method further comprises restoring data to the source storage device from the computer readable medium.

20. (Canceled)

21. (Original) The computer readable storage medium of claim 17, wherein the method further comprises storing and transporting data in the accessible portion of the computer readable medium.

22. (Previously Presented) A method for secure computer readable medium backup, the method comprising:

providing a computer readable medium having at least a first accessible portion and a second encrypted portion;

initializing a password module in response to verifying a cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module;

transmitting an encrypted password to the cryptographic module;

authenticating the encrypted password;

decrypting the encrypted password;

transmitting the decrypted password to the computer readable medium; and

decrypting the second encrypted portion using the decrypted password.

23. (Original) The method of claim 22, further comprising copying data from a source storage device, and storing the data in the second encrypted portion of the computer readable medium.

24. (Original) The method of claim 22, further comprising restoring data to the source storage device from the computer readable medium.

25. (Canceled)

26. (Original) The method of claim 22, further comprising storing and transporting data in the accessible portion of the computer readable medium.

27. (Previously Presented) An apparatus for secure computer readable medium backup, the apparatus comprising:

means for providing a computer readable medium having at least a first accessible portion and a second encrypted portion;

means for initializing a password module in response to verifying a cryptographic module by comparing a known value stored on the password module to a cryptographic module platform configuration register value storing a hash of POST BIOS code, wherein only the cryptographic module may initialize the password module;
means for transmitting an encrypted password to the cryptographic module;
means for authenticating the encrypted password;
means for decrypting the encrypted password;
means for transmitting the decrypted password to the computer readable medium module; and
means for decrypting the second encrypted portion using the decrypted password.

28. (Original) The apparatus of claim 27, further comprising means for copying data from a source storage device, and storing the data in the second encrypted portion of the computer readable medium.

29. (Original) The apparatus of claim 27, further comprising restoring data to the source storage device from the computer readable medium.

30. (Canceled)

Ellen Tran
ELLEN TRAN
PATENT EXAMINER
ART 2134